



HIPAA Privacy & Security Crosswalk

HIPAA Privacy and Security Defined

PRIVACY

- Controlling who is authorized to access information and how those persons use and disclose the information.
- Privacy is not only an I.T. function. It is also the responsibility of the healthcare entities administration because it deals with how an organization defines and implements policies.
- *Privacy is the right of individuals to keep information about themselves from being disclosed.*

SECURITY

- The ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss.
- Data security is more reliant on IT solutions and should be the primary responsibility of the IT department in conjunction with facility operations.
- *Security applies to the spectrum of physical, technical and administrative safeguards that are put in place to protect the integrity, availability and confidentiality of information.*

Who Must Comply?

PRIVACY

- All health plans, clearinghouses, and healthcare providers that electronically store or transmit individual health information must comply.

SECURITY

- All health plans, clearinghouses, and healthcare providers that electronically store or transmit individual health information must comply.

Enforcement Authority

PRIVACY

- HHS Office for Civil Rights (OCR) will oversee and enforce privacy requirements including:
 - Imposing civil penalties
 - Making referrals for criminal prosecution
 - Making exception determinations
 - Overseeing voluntary compliance
 - Responding to questions regarding the rules and providing interpretation and guidance
 - Responding to state requests or exception determinations.

SECURITY

- HHS officials announced on October 15 that the Centers for Medicare & Medicaid Services (CMS) will establish and operate the enforcement process for the security standards.

Compliance Deadlines

PRIVACY

- Privacy Rule compliance is required by April 14, 2003 for most covered entities (small health plans have until 04/14/04 to comply with the rule).

SECURITY

- The Proposed Security Rule has yet to be finalized. Standards are required to be implemented generally within two years of the effective date of the final rule. The effective date of the final rule is generally 60 days after its publication. Therefore, the compliance deadline for the proposed security rule will not likely be before February, 2005.

Privacy and Security Requirements

PRIVACY

- The Privacy rule lists 58 Privacy requirements.

SECURITY

- The Security NPRM lists 24 proposed Security requirements.
- 12 of the proposed Security requirements are also addressed in the Privacy rule.

Common Privacy and Security Requirements

- Contracts with business partners
- Record Processing
- Access controls
- Incident procedures
- Security / privacy management
- Sanctioning
- Training
- Assigned responsibility – HIPAA officer
- Physical access controls
- Internal Audit
- Authorization controls
- Personnel Security

Contracts With Business Partners

PRIVACY

Establish Business Associate agreements between the covered entity and its business partners who will be using or disclosing the entity's Protected Health Information for purposes other than treatment.

SECURITY

Entities must establish Chain of Trust Partner Agreements between other entities with whom health information is shared, to "protect the integrity and confidentiality" of the data they exchange.

Record Processing

PRIVACY

Policies and procedures must be established for the use and disclosure of Protected Health Information. Documentation of privacy policies, authorizations, complaints, sanctions, etc. must be completed and maintained for six years.

SECURITY

Policies and procedures must be established for the receipt, handling and disposal of health information (for cradle to grave processing).

Access Controls

PRIVACY

All covered entities must request or disclose only the minimum necessary Protected Health Information (PHI) to accomplish the purpose for which the information is requested or needed.

SECURITY

Covered entities must provide controls limiting access to health information to those with valid needs and authorization.

Incident Procedures

PRIVACY

A covered entity must mitigate any harmful effect that is known from an inappropriate release of Protected Health Information.

Entities should implement administrative, technical, and physical safeguards to prevent breach of privacy.

SECURITY

Establish measures for reporting and responding to security incidents.

Security / Privacy Management

PRIVACY

Entities must establish policies pertaining to Protected Health Information to address the full range of privacy issues to include:

- Risk analysis
- Implementation procedures
- Complaint process
- Appropriate sanctions

SECURITY

Requires a covered entity to have a formal security management process in place to address the full range of security issues to include:

- Risk analysis
- Risk management
- Sanctions policy
- Security policy

Sanctioning

PRIVACY

Develop and apply appropriate sanctions against employees who fail to comply with the privacy policies and procedures.

SECURITY

Develop policies regarding disciplinary actions for violations of security policies and procedures and communicate to all employees.

Training

PRIVACY

Staff training concerning the privacy rule and the policies pertaining to the rule must be completed prior to the compliance date.

SECURITY

Security training must be conducted for all staff that covers security awareness, periodic reminders, password management, virus protection and monitoring login success/failure.

Assigned Responsibility – HIPAA Officers

PRIVACY

Assignment of a Privacy Officer. This individual is to have responsibility for implementation and compliance.

SECURITY

Assignment of a Security Officer – This individual is assigned responsibility for maintaining the security of electronic patient data.

Physical Access Controls

PRIVACY

Requires entities to establish, as appropriate, administrative, technical and physical safeguards to protect the privacy of Protected Health Information.

SECURITY

Entities must develop a facility security plan, and set up disaster recovery, emergency operations, and other access and handling controls.

Internal Audit

PRIVACY

Disclosures of Protected Health Information for purposes other than treatment, payment, and operations must be documented and maintained for six years.

SECURITY

Covered entities are required to set up system mechanisms that record and monitor activity.

Authorization Controls

PRIVACY

A patient authorization must be obtained to disclose Protected Health Information (PHI) for purposes other than treatment, payment and operations.

Under certain limited “permitted use” conditions, PHI may be disclosed without patient authorization.

SECURITY

Entities must obtain and track the consents of patients for use and disclosure of their health information.

Personnel Security

PRIVACY

The covered entity must identify the classes of persons who need access to PHI, including the conditions of such access, and limit access accordingly.

SECURITY

Entities should ensure that personnel are authorized to access Protected Health Information. Entities must:

- Obtain appropriate clearances
- Supervise maintenance personnel
- Maintain records of access authorizations
- Secure proper authorizations for operating and maintenance personnel
- Develop personnel security policies and procedures

What's in the Security NPRM.... But not in the Privacy rule?

- Certification
- Contingency Plans
- Security Configuration Management
- Termination Procedures
- Media Controls
- Workstation use
- Workstation location
- Audit controls
- Data authentication
- Entity authentication
- Communications /network controls

Certification

Covered entities must obtain a formal statement that the organization is in compliance with the security standards. The proposed Security rule does not specify where such certification is to be obtained.

Contingency Plans

- Covered entities are required to:
- Perform periodic backups of data
- Develop plans for continued operation of critical facilities / functions
- Establish disaster recovery procedures

Security Configuration Management

Covered entities are required to implement measures, practices, and procedures for the security of information to include:

- Document the security policies and procedures
- Coordinate and integrate procedures with other practices
- Periodically test security features
- Review hardware installation and maintenance records
- Inventory hardware / software
- Install and maintain virus software

Termination Procedures

Entities must document procedures for terminated employees to:

- Remove employees from access list
- Deactivate user accounts
- Retrieve keys, badges, or other access cards

Media Controls

Covered entities are required to document policies and procedures for:

- Access Control; the receipt of hardware and/or software
- Data Disposal; the removal of hardware and/or software
- Accountability; tracking hardware and software into and out of a facility

Workstation Use

Workstation instructions and procedures should be developed to include:

- Logging off after use
- Password-protected screen savers
- Password changes

Workstation Location

- Entities must protect workstations from unauthorized use.
- Implementation strategies may include:
 - Screen savers
 - Computer locks
 - Secured offices
 - Automatic logoffs

Audit Controls

- Entities should establish mechanisms to record and examine system activity to:
 - Identify suspect data access activities
 - Assess the security program
 - Respond to potential weaknesses

Data Authentication

- Entities must demonstrate that data has not been altered in an unauthorized manner.
- Techniques may include:
 - Check sum
 - Double keying
 - Message authentication code
 - Digital signature

Entity Authentication

- Entities seeking to access protected data must be able to prove their identity
- Authentication MUST include both:
 - Automatic logoff
 - Unique user identification
- Authentication MUST also include one of the following:
 - Biometric identification
 - Passwords
 - PINs
 - Telephone callback
 - Tokens

Communications / Network Controls

■ Requirements for networks used for communication:

- Alarm
- Audit Trail
- Entity authentication
- Event reporting

■ Requirements for all networks:

- Integrity controls
- Message authentication
- Access controls OR encryption

Should Entities Wait to Implement Security?

- The Dilemma:
- What privacy concerns may be compromised by waiting for the final security rule?
- Should entities fund two projects?
- Will it be less expensive to just implement the Privacy rule?
- What will be the additional costs to implement the security requirements once compliance with the Privacy rule has been met?
- Possibilities:
- Privacy compliance may not be attainable without some security features.
- Costs savings of two implementations may not be realized.
- Entities may spend more to fund two implementations.

Risks of Delaying the Security Requirements

- Additional costs for two implementations
- Non-compliance with the privacy rule due to inadequate security measures
- Added information security risk to the organization as the privacy requirements are implemented.

Recommendations

- Conduct privacy and security assessments simultaneously to determine all risks
- Develop implementation strategies to incorporate both privacy and security:
 - Prioritize those requirements that overlap
 - Determine the security requirements that will yield cost savings by implementing them along with privacy
 - Determine the “risks” associated with a delay in implementing the proposed security requirements including:
 - Risks in securing Protected Health Information
 - Legal and Financial implications

OTHER SECURITY CONSIDERATIONS

IT security best practice benchmarks...

Available to the health care sector

DoD can obtain and apply these guidelines right away to their strategic HIPAA security strategic program. Source examples include:

Source	Value
Department of Health and Human Services HIPAA Security and Electronic Signature Standards (Proposed Rule)	HIPAA implementation requirements: •Organizational Practices •Technical Practices and Procedures •Security requirements in four categories (Administrative, Physical, Technical Services, Technical mechanisms) •References many other standards
Government Information Security Reform Act (GISRA)	Requires all government agencies to: •Implement an agency-wide information security program •Conduct annual reviews of the program •Implement incident response capability •Include program descriptions and schedules in the annual performance plan •Report deficiencies in policies or practice
Guidelines for the Management of IT Security (ISO/IEC 13335)	Best-practice guidance from the International Standards Organization with individual volumes on: •Concepts and models for IT Security. •Managing and planning IT Security. •Techniques for the management of IT Security. •Selection of safeguards.
NRC Report: <i>For the Record: Protecting Electronic Health Information</i> (1997)	Describes technological & organizational aspects of security management. Provides guidance on protecting health information, including recommendations for technical and organizational solutions. The real challenge is not in defining “what” to do in the general sense, but in actually implementing change in the organization.

Some common mistakes of IT security management

- Undervalued Information. Few organizations analyze the contributions that specific information assets make to the bottom line.
- Lack of risk management processes. Because organizations often have no institutionalized means of evaluating threats and vulnerabilities, the security implications of corporate procedural changes, or the likelihood and impact of IT security-related risks.
- Narrowly defined security boundaries. Organizations focus internally, neglecting to evaluate and understand the security practices of their business partners.
- Dated security management processes. Security managers often mistakenly view security risks as static, when in fact they change constantly as the organization, network configuration, and technology change.
- Lack of communication about security responsibilities. Security is viewed as an exclusively technical issue, and is thought to be the purview of the information systems organization. Security is everyone's responsibility, and the greatest challenges are usually not the technical ones.
- Crisis-driven security. A reactive approach to security permits serious damage to the organization and ignores risks that have not yet caused harm.
- Poor security awareness and training. Technical personnel knowledge and skills become dated, and other staff members are not sufficiently informed of security risks and good practices.